

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A computer controlled method in a provisioning
- 2 device in a networked computer system comprising an execution mechanism
- 3 configured to execute the method, the method comprising:
 - 4 establishing communication between the provisioning device and the
 - 5 network device over a preferred channel, wherein the preferred channel is a
 - 6 location-limited channel which has a demonstrative identification property and an
 - 7 authenticity property;
 - 8 exchanging key commitment information over said preferred channel
 - 9 between said provisioning device and said network device to pre-authenticate said
 - 10 network device;
 - 11 providing provisioning information to said network device over said
 - 12 preferred channel, wherein the provisioning information comprises:
 - 13 a first set of provisioning information which is used exclusively to
 - 14 establish secure and authenticated communication between the
 - 15 provisioning device and the said network device using a second channel,
 - 16 wherein the second channel need not be location-limited; and
 - 17 other provisioning information;
 - 18 wherein the first set of provisioning information is provided over
 - 19 the preferred channel, and the other provisioning information is provided
 - 20 using a second channel, and

21 whereby said network device can automatically configure itself for secure
22 communication over a network responsive to said first and other provisioning
23 information, wherein the secure communication can be over the second channel.

1 2. (Original) The computer controlled method of claim 1, wherein said
2 provisioning information comprises network configuration information.

1 3. (Original) The computer controlled method of claim 1, further comprising
2 receiving a public key from said network device;
3 verifying said public key with said key commitment information; and
4 automatically provisioning said network device with a credential
5 authorized by a credential issuing authority.

1 4. (Original) The computer controlled method of claim 3, further comprising
2 establishing proof that said network device is in possession of a private
3 key corresponding to said public key.

1 5. (Original) The computer controlled method of claim 3, wherein said
2 credential issuing authority is a certification authority and said credential is
3 a public key certificate.

1 6. (Original) The computer controlled method of claim 3, wherein the step of
2 automatically provisioning is responsive to authorization from a
3 registration agent.

1 7-8 (Canceled).

1 9. (Original) The computer controlled method of claim 1, wherein the
2 network is a wireless network, and wherein said provisioning device is a
3 wireless access point.

1 10. (Original) The computer controlled method of claim 9, further comprising:
2 receiving a wireless communication;
3 determining whether said wireless communication originated from
4 said network device or from a second network device that was not
5 provisioned by said wireless access point; and
6 routing said wireless communication responsive to the step of
7 determining.

1 11. (Original) The computer controlled method of claim 10, wherein the step
2 of routing comprises:
3 choosing a selected channel from a secure channel and an insecure
4 channel responsive to the step of determining; and
5 sending said wireless communication through said selected channel.

1 12. (Original) The computer controlled method of claim 1, wherein said
2 provisioning device is in communication with a credential issuing
3 authority.

1 13. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method to provision a network device, the method comprising steps of:
4 establishing communication between the provisioning device and
5 said network device over a preferred channel, wherein the preferred

6 channel is a location-limited channel which has a demonstrative
7 identification property and an authenticity property;
8 exchanging key commitment information over said preferred channel
9 between said provisioning device and said network device to pre-
10 authenticate said network device;
11 providing provisioning information to said network device over
12 said preferred channel, wherein the provisioning information comprises:
13 a first set of provisioning information which is used exclusively to
14 establish secure and authenticated communication between the
15 provisioning device and the said network device using a second channel,
16 wherein the second channel need not be location-limited; and
17 other provisioning information;
18 wherein the first set of provisioning information is provided over the
19 preferred channel, and the other provisioning information is provided
20 using a second channel, and
21 whereby said network device can automatically configure itself for
22 secure communication over a network responsive to said first and other
23 provisioning information, wherein the secure communication can be over
24 the second channel.

1 14. (Original) The computer-readable storage medium of claim 13, further
2 comprising
3 receiving a public key from said network device;
4 verifying said public key with said key commitment information; and
5 automatically provisioning said network device with a credential
6 authorized by a credential issuing authority.

1 15. (Original) The computer-readable storage medium of claim 13, wherein
2 the network is a wireless network, and wherein said provisioning device is
3 a wireless access point.

1 16. (Currently amended) An apparatus for provisioning a network device
2 comprising:

3 at least one port configured to establish a preferred channel;
4 a preferred communication mechanism configured to be able to
5 establish communication with and said network device over said
6 preferred channel, wherein the preferred channel is a location-limited
7 channel which has a demonstrative identification property and an
8 authenticity property;

9 a pre-authentication mechanism configured to be able to receive key
10 commitment information over said preferred channel from said network
11 device;

12 a provisioning mechanism configured to provide provisioning
13 information to said network device, wherein the provisioning information
14 comprises:

15 a first set of provisioning information which is used
16 exclusively to establish secure and authenticated communication between
17 the provisioning device and the said network device using a second
18 channel, wherein the second channel need not be location-limited; and

19 other provisioning information;

20 wherein the first set of provisioning information is provided
21 over the preferred channel, and the other provisioning information
22 is provided using a second channel; and

23 whereby said network device can automatically configure itself for
24 secure communication over a network responsive to said first and other
25 provisioning information, wherein the secure communication can be over
26 the second channel.

1 17. (Original) The apparatus of claim 16, wherein said provisioning
2 information comprises network configuration information.

1 18. (Original) The apparatus of claim 16, further comprising
2 a key reception mechanism configured to receive a public key;
3 a key verification mechanism configured to verify said public key
4 with said key commitment information; and
5 a credential provisioning mechanism configured to automatically
6 provide a credential authorized by a credential issuing authority.

1 19. (Original) The apparatus of claim 18, further comprising a key exchange
2 mechanism configured to be able to perform a key exchange protocol with
3 said network device.

1 20. (Original) The apparatus of claim 18, wherein said credential issuing
2 authority is a certification authority and said credential is a public key
3 certificate.

1 21-22 (Canceled).

1 23. (Original) The apparatus of claim 22, further comprising:

2 a packet receiver mechanism configured to receive a wireless
3 communication;
4 a determination mechanism configured to determine whether said
5 wireless communication received by the packet receiver mechanism
6 originated from said network device or from a second network device that
7 was not provisioned by said wireless access point; and
8 a router mechanism configured to route said wireless communication
9 responsive to the determination mechanism.

1 24. (Original) The apparatus of claim 23, wherein the router mechanism
2 further comprises:
3 a channel selection mechanism configured to choose a selected
4 channel from a secure channel and an insecure channel responsive to the
5 determination mechanism; and
6 a transmission mechanism configured to send said wireless
7 communication through said selected channel.

1 25. (Original) The apparatus of claim 16, further comprising a non-preferred
2 communication mechanism that can be used to communicate with a
3 credential issuing authority.

1 26-66. (Canceled)